CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ATIC-213-2019
17-12-2019

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2019 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar la gestión de la configuración en equipo de redes y comunicaciones a nivel institucional, específicamente en centros de gestión informática del ámbito local y regional.

En ese sentido, los resultados del informe permitieron evidenciar la ausencia de normativa orientada de manera específica a la gestión de la configuración a efectuarse en equipamiento de telecomunicaciones, esto en aras de garantizar la integridad de las disposiciones de hardware y software aplicadas en los componentes citados de la plataforma tecnológica.

En concordancia con lo anterior, se comprobó la necesidad de la Institución en mejorar la disponibilidad y completitud de la documentación utilizada para evidenciar los elementos considerados por el personal informático en atención al funcionamiento de la red local que administran, esto desde la disposición de la Línea Base de Configuración, cambios efectuados y mejoras aplicadas.

Lo descrito en párrafos anteriores evidenció debilidades en aspectos asociados a seguridad informática, las cuales están relacionadas al monitoreo y supervisión sobre los dispositivos, establecimiento de contraseñas seguras, creación de perfiles de acceso y la generación de respaldos; elementos que buscan asegurar razonablemente integridad de la configuración actual de los equipos de redes y comunicaciones, no obstante, esas vulnerabilidades podrían amenazar la continuidad de los servicios TI.

Finalmente, se comprobó la necesidad de fortalecer los procesos de capacitación y concientización referente a este tema en la Caja, lo cual contribuiría eventualmente con la disminución de prácticas no alineadas las mejores metodologías que refieren sobre esta materia.

En virtud de lo expuesto, este Órgano de Fiscalización ha solicitado a la Administración Activa, se adopten acciones concretas para la atención a las recomendaciones insertas en el presente informe.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ATIC-213-2019
17-12-2019

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ESTUDIO DE CARÁCTER ESPECIAL SOBRE LA GESTIÓN DE LA CONFIGURACIÓN EN EQUIPO DE REDES Y COMUNICACIONES A NIVEL INSTITUCIONAL
DIRECCION DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo del 2019 para el Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la Gestión de la Configuración en equipo de Redes y Comunicaciones de acuerdo con lo establecido en la normativa de la Caja Costarricense del Seguro Social (CCSS).

OBJETIVOS ESPECÍFICOS

1. Determinar el establecimiento formal de regulación a nivel institucional sobre la gestión de la configuración en equipamiento de redes y comunicaciones.
2. Revisar la documentación que respalda la configuración aplicada en los dispositivos de telecomunicaciones.
3. Comprobar la aplicación de buenas prácticas de seguridad informática en los temas correspondientes a gestión de la configuración.
4. Verificar la gestión de la configuración efectuada como parte de las actividades definidas para la administración de la red en el nivel regional y local en torno al monitoreo de los dispositivos e interacción de los equipos con terceros.
5. Identificar la disposición de capacitación y/o conocimientos del personal destacado en los Centros de Gestión Informática regionales y locales, relacionado a la administración de la configuración en equipo de redes y comunicaciones.

ALCANCE

El estudio comprende todas aquellas acciones efectuadas por parte de la Administración Activa en torno a la gestión de configuración en equipo de redes y comunicaciones en el ámbito de los Centros de Gestión Informática regional y local, durante el periodo comprendido entre enero del 2019 y noviembre del 2019.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Con el propósito de alcanzar los objetivos propuestos, se desarrollaron los siguientes procedimientos metodológicos:

- Revisión y análisis de información suministrada por la Administración Activa referente a la gestión de configuración en equipamiento de redes y comunicaciones de los sitios.

- Entrevista y/o reuniones efectuadas con los siguientes funcionarios:

  - Máster Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas.
  - Licda. Jeannette Madrigal Loría, Jefe de Subárea de Soporte a Comunicaciones.
  - Lic. Douglas Marín Mendoza CGI, Dirección Regional de Servicios de Salud Chorotega
  - Lic. Jimmy Ortiz Duarte, CGI, Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte.
  - Lic. Jorge Paniagua Pérez , CGI, Dirección Regional Sucursales Brunca
  - Lic. Rafael A. Alvarez Rodríguez, CGI, Dir. Reg. Central de Sucursales.
  - Licda. Carmen Suárez González, CGI, Hospital Dr. Carlos Luis Valverde Vega.
  - Lic. Emanuel Arrieta Loáiciga, CGI, Hospital Dr. Enrique Baltodano Briceño.
  - Licda. Jency Raquel Alpízar Rodríguez, CGI, Hospital de San Vito.
  - Licda. Jimmy Andrés Salazar Arrieta, CGI, Hospital San Carlos.
  - Lic. John Harold Vega Gómez, CGI, Hospital Ciudad Neilly.
  - Lic. Rafael Porras Murillo, CGI, Hospital Tomas Casas Casajus.
  - Lic. Alexánder Centeno Quirós, CGI, Área De Salud Cañas.
  - Lic. Alvaro Alvarado Espinoza, CGI, Área de Salud de Tilarán
  - Lic. Jeffry Vinicio Alvarez Rojas, Área Salud de Buenos Aires
  - Lic. Herschel Alberto Jiménez Barahona, CGI, Área de Salud de Naranjo
  - Licda. Sirleny Barrantes Valverde, CGI, Area Salud Coto Brus

MARCO NORMATIVO

- Ley No. 8292 – Ley General de Control Interno, CR.
- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) No. R-CO-9-2009.
- Normas Técnicas para la Gestión y Control de Tecnologías de Información, CGR.
- Normas Institucionales en Tecnologías de Información y Comunicaciones.
- Políticas Institucionales de Seguridad Informática, CCSS.
- Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones.
- Manual de Organización de los Centros de Gestión Informática (CGI).
- Guía técnica para gestión de procesos de mantenimiento preventivo y correctivo en routers y switches, TIC-COM-0003, Versión 1.0.0 Octubre 2014.

ASPECTOS RELACIONADOS CON LA LEY GENERAL DE CONTROL INTERNO

Esta Auditoría informa y previene al Jerarca y a los titulares subordinados acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37, 38 de la Ley No. 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"(…) Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)".*

ANTECEDENTES

El desarrollo tecnológico que se ha venido presentando durante las últimas décadas ha logrado avanzar de manera vertiginosa en comparación con años anteriores, parte de ese crecimiento corresponde a la modernización en el ámbito informático al que se exponen las telecomunicaciones, las cuales reaccionan de manera acelerada.

Es decir, las telecomunicaciones consisten en múltiples estaciones de receptores y transmisores que intercambian información entre sí. Esto incluye tecnologías como radio, telefonía, comunicaciones de datos y redes informáticas, mediante las cuales es posible brindar servicios de voz, video y datos, entre otros, los cuales constituyen un medio de comunicación integral y convergente.

En ese sentido, equipamiento de switches, routers, firewalls y otros equipos, catalogados como hardware, permiten las comunicaciones entre diversos dispositivos que existen en una red, así como establecer la conexión con un Proveedor de Servicios de Internet -ISP, con siglas en inglés- y con ello propiciar conectividad a Internet.

Cabe agregar que dichos dispositivos se encuentran sujetos a configuraciones, las cuales establecen la forma en que funcionarán los elementos físicos y lógicos dentro de la plataforma tecnológica, esto mediante los valores que el administrador de la red considere pertinente aplicar en los dispositivos, con base a las necesidades y características en donde se instalará el equipo.

Es decir, esa gestión podría derivarse en dos grandes áreas, la primera de ellas la que corresponde a la configuración inicial de los equipos (sea predeterminada o personalizada) y en una segunda instancia los cambios efectuados a partir de los parámetros establecidos anteriormente.

Dicha gestión incluye entre otros aspectos el manejo de versiones y actualizaciones aplicados a los paquetes de software instalados en los equipos, ubicación y direcciones de red de los dispositivos de hardware, lo anterior, en aras de asegurar continuidad de servicios antes cambios o restauraciones del sistema puedan ser realizados sin afectar negativamente a cualquiera de los sistemas y/o usuarios.

Marco de Referencia sobre las mejores prácticas relacionadas al tema

Al respecto, entre las mejores prácticas que identifican la importancia de gestionar la configuración, se encuentra el marco de referencia ITIL®, en el cual uno de los 26 procesos se denomina "Gestión de la Configuración y Activos del Servicio", destacando entre sus funciones lo siguiente:

- Llevar el control de todos los elementos de configuración de la infraestructura TI con el adecuado nivel de detalle y gestionar dicha información a través de la Base de Datos de Configuración.
- Proporcionar información precisa sobre la configuración TI a la Planificación y Soporte a la Transición ante posibles coordinaciones que requieran cambios, para que ésta pueda establecer las fases y plazos en que se articulará la transición.
- Apoyar la interacción con la gestión de incidencias, problemas, cambios y entregas y despliegues de manera que éstas puedan resolver más eficientemente las incidencias, encontrando rápidamente la causa de los problemas, realizando los cambios necesarios para su resolución y mantener actualizada en todo momento la Base de Datos de Configuración.
- Monitorizar periódicamente la configuración de los sistemas en el entorno de producción y contrastarla con la almacenada en la Base de Datos de Configuración para subsanar discrepancias.

ATIC -76-2018 "Evaluación de la gestión de las telecomunicaciones a nivel Institucional",

Dentro de los antecedentes, este ente fiscalizador mediante el informe ATIC -76-2018 "Evaluación de la gestión de las telecomunicaciones a nivel Institucional", evidenció oportunidades de mejora en la administración de la plataforma tecnológica utilizada para las telecomunicaciones, en aspectos como el cumplimiento de las funciones establecidas en el marco normativo aplicable, así como la necesidad del uso eficaz y eficiente de las tecnologías de manera integral para alcanzar el cumplimiento de la estrategia plasmada por la Caja Costarricense del Seguro Social.

Adicionalmente indicando recomendaciones sobre las mejoras a efectuar en los mecanismos utilizados para evaluar y dar seguimiento a los actores involucrados en la gestión de las redes y comunicaciones, esto mediante las normativas que se establecieron para regular la gestión de las telecomunicaciones, en aras de garantizar la obtención de los beneficios asociados al desarrollo de la gestión a nivel Institucional.

Por otra parte, en relación con los servicios que ofrece Área de Comunicaciones y Redes Informáticas, se identificó que carecen de participación en iniciativas de adquisición de equipamiento y servicios, falencias en la implementación y monitoreo de enlaces de comunicaciones y otras características que dispone la red, particularmente en aspectos tales, indicadores de gestión, elaboración de estudios técnicos y factibilidad, gestión de tráfico en la red, estrategias de cobertura instalada y migración de la telefonía, estandarización en la gestión de incidencias, entre otros factores que determinan el rendimiento y la disposición de estos.

Finalmente, entre otros se indicaron aspectos asociados a la administración del equipamiento debido a que no se realizan diagnósticos situacionales donde se valore el estado actual de la plataforma tecnológica que soporta las telecomunicaciones en los sitios, además, en lo que respecta a las inversiones para la adquisición de equipo y servicios, donde se observaron acciones que no responden a las necesidades actuales que refieren las unidades.

Situación Actual

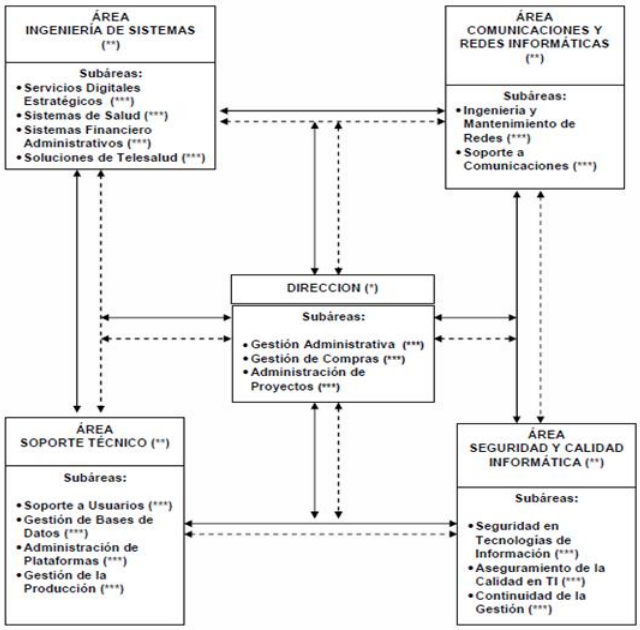
Por consiguiente, la CCSS por medio de activos tecnológicos asociados a la redes y comunicaciones, soporta las operaciones y servicios de TIC siendo necesario la gestión de la configuración antes citada, en aras de responder a las expectativas del negocio y de los usuarios.

No obstante, la complejidad de la Caja Costarricense del Seguro Social demanda interacción eficaz y eficiente para gestionar recursos y capacidades al entregar servicios de redes informáticas acorde a lo esbozado anteriormente. Ahora bien, en representación de la cobertura en telecomunicaciones a nivel institucional, a mayo 2017, se identificaron 1095 enlaces reportados por el Área de Comunicaciones y Redes Informáticas (ACRI), de los cuales un 97,17% (994) disponían de al menos un enlace de comunicaciones, mientras que esos indicadores mostraron un incremento de un 5,3% respecto al año 2015, situación que demuestra la necesidad de disponer de una gestión integrada de la configuración acorde a nuestra infraestructura tecnológica.

En ese sentido, los actores a nivel Institucional que participan en las labores antes mencionadas se designaron por la Junta Directiva, mediante el artículo No. 44 de la sesión No. 8555 de fecha 26 de enero de 2012, en la cual se dio la aprobación del Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, definiéndose entre otros aspectos, las funciones sustantivas del ACRI y la conformación de esa Área en dos subáreas adscritas, a saber:

- Subárea Soporte a Comunicaciones
- Subárea Ingeniería y Mantenimiento de Redes

Figura 1
Niveles organizacionales presentes en la Dirección de Tecnologías de Información y Comunicaciones.



Fuente: Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, 2013, p.50.

Así mismo, el objetivo del ACRI descrito en el Manual de Organización mencionado es:

"…Garantizar el funcionamiento óptimo de la infraestructura de comunicaciones a nivel interno y en las unidades fuera de Oficinas Centrales (Red WAN) y transmisión de voz, video y datos. Otorga el soporte técnico requerido en materia de redes computacionales, protocolos e infraestructura de comunicación de datos. Es responsable de la administración, soporte, asesoría y configuración de los equipos de comunicación disponibles en la Institución y de la gestión ante el ICE para la conexión de las unidades, esta actividad permite mantener un control de los requerimientos de comunicación y es el responsable de gestionar y reportar problemas ante el ICE. Por su naturaleza debe mantener una relación constante con diversas unidades de trabajo…".

Posteriormente, en agosto del 2015 se establecieron los Lineamientos en Comunicaciones y Redes Informáticas, las cuales definen para esta unidad la siguiente función:

"…Le corresponde al Área de Comunicaciones y Redes Informáticas (ACRI), de la Subgerencia de Tecnologías de Información y Comunicaciones (STIC), liderar el diseño e implementación de la red de comunicaciones institucional, mediante una gestión de coordinación, investigación, asesoramiento y valoración de proyectos en la materia, que den como producto, un desarrollo integral y armónico de las redes de comunicaciones institucionales.

Igualmente, el Área de Comunicaciones y Redes Informáticas debe velar por el buen funcionamiento y disponibilidad de las redes de comunicaciones a nivel institucional, estableciendo políticas, estrategias y normas, con el fin de disponer de mecanismos de coordinación para la adquisición, implementación y mantenimiento de la infraestructura de comunicaciones y redes informáticas, con el objetivo de asegurar la maximización de los recursos entorno al ámbito de las redes y comunicaciones, para el cumplimiento de la visión y misión de la Institución…"

Aunado a lo anterior, otro autor que interactúa en este tema son los Centros de Gestión Informática (CGI), según lo establece en el Manual de Organización de ese nivel organizacional, indica como un objeto especifico:

"Mantener en óptimo estado de funcionamiento las redes de comunicación y la tecnología I.P."

Además, en ese mismo cuerpo normativo se regula la participación de los CGI en iniciativas que refieran a telecomunicaciones, según lo indica el apartado "Conceptualización del Centro de Gestión Informática", citando lo siguiente:

"Es responsable de realizar las actividades operativas que apoyan el desarrollo de las tecnologías de información y comunicaciones, la ejecución de estudios de necesidades, la automatización de procesos estratégicos y operativos, participa activamente en la elaboración de planes, la administración de proyectos el desarrollo de los sistemas automatizados, implementa los mecanismos de coordinación, de comunicación, aplica las nuevas tecnologías, administra los equipos y las redes de información en su ámbito de competencia; es un enlace entre los usuarios no especializados, la Dirección de Tecnologías de Información y Comunicaciones y otros órganos competentes."

Así mismo, en ese mismo cuerpo normativo se establece dentro de las funciones del Centro de Gestión Informática Regionales y Locales, lo siguiente:

> *"Administrar los dispositivos de comunicaciones en su ámbito de acción, conforme con las políticas y estándares definidos, con el propósito de asegurar la comunicación efectiva de los sistemas de información."*

En particular, la Institución dispone de funcionarios en los Centros de Gestion Informática, los cuales brindan soporte en sitio para administrar la red, incluyéndose el tema supra citados, así como atender eventuales interrupciones a la continuidad de las redes y comunicaciones, de acuerdo con el ámbito de acción, responsabilidades y niveles de resolución, entre otros factores a considerar.

Debido a lo anterior, se detallan a continuación los hallazgos evidenciados por esta Auditoría en torno a riesgos detectados en la gestión de configuración para equipamiento de telecomunicaciones a nivel Institucional.

HALLAZGOS

1. SOBRE LA NORMATIVA REFERENTE A LA GESTIÓN DE CONFIGURACIÓN

Se determinó la ausencia de normativa orientada a regular la gestión de la configuración en equipo de telecomunicaciones, en la cual se considere las actividades y responsabilidades correspondientes tanto al nivel interno, como ante la participación de terceros.

En ese sentido, se constató mediante consulta efectuada a 15 unidades programáticas destacadas en el I y II nivel de atención, Direcciones de Red Integrada de Prestación de Servicios de Salud, Direcciones Regionales de Sucursales y unidades adscritas, específicamente lo concerniente a la gestión de configuración en los equipos antes citados.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el apartado 5.1 Seguimiento de los procesos de TI y Seguimiento y evaluación del control interno en TI, citan lo siguiente:

> *"**5.1 Seguimiento de los procesos de TI**. La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso. "*
>
> ***"5.2 Seguimiento y evaluación del control interno en TI.** El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas."*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Comunicaciones y Redes Informáticas establece:

> *"[…]Formular, actualizar y evaluar la regulación, la normativa técnica, los protocolos y estándares relacionados con su ámbito de acción, en respuesta a la normativa aprobada por el Consejo de Presidencia y de Gerentes, la tecnología en uso y los procesos de investigación, con el propósito de lograr uniformidad en los sistemas y maximización de los recursos institucionales."*
>
> *"[…]Actualizar la documentación técnica en su ámbito de competencia, con base en los requerimientos de la organización, las políticas y estrategias vigentes, con el objeto de lograr la operación efectiva del hardware y software institucional."*

Ese mismo cuerpo normativo indica como función sustantiva de la Subárea de Ingeniería y Mantenimiento de Redes y de la Subárea de Soporte a Comunicaciones, lo siguiente:

> *"[…]Participar en la formulación, actualización y evaluación de la regulación, la normativa técnica, proponer los protocolos y estándares en su ámbito de competencia, de acuerdo con los procesos de investigación y los requerimientos institucionales, con el propósito de lograr el desarrollo efectivo de la gestión."*

Las Normas Institucionales en Tecnologías de Información y Comunicaciones establece en su artículo 3.3.2 "En cuanto a Infraestructura de Redes y Comunicaciones", lo siguiente:

> *"…Corresponde a la Dirección de Tecnologías de Información y Comunicaciones asesorar y mantener vigente la normativa y especificaciones técnicas en esta materia…"*

Al respecto, el MSc. Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas, refiriéndose a la actualización de la normativa existente, indicó lo siguiente:

> *"actualmente existen lineamientos que refieren a la gestión propia de telecomunicaciones qué son las que han estado publicadas hasta el momento. Además de esos lineamientos, existen los manuales de organización, tanto para nuestra área como para los centros de gestión informática, los cuales indican el ámbito de competencia para cada caso, esa es la única referencia nuestra a esos temas.*
>
> *Ahora bien, dicho cuerpo normativo no es específico para detallar las tareas o actividades que pueden ser consideradas como parte de la gestión integrada o articulada de la configuración en equipamiento de redes y comunicaciones.*
>
> *Las guías que hemos emitido para abordar parcialmente el tema podrían ser a manera de ejemplo: Guía de implementación: Redes inalámbricas de ámbito local (WLAN) DTI-I-MR-0006, Marco de referencia para el diseño de alta disponibilidad en redes hospitalarias (componentes activos), Guía para la medición del rendimiento y monitoreo de la red LAN, Guía de referencia para proyectos de Cableado Estructurado y otros componentes, Marco Técnico de referencia de Cableado Estructurado.*

En ese sentido, la documentación podría considerarse parte del apoyo (asesoría recomendativa) que brindamos, no obstante, reitero que a pesar de no disponer de lineamientos específicos para el tema como tal, nuestra apertura para asesorar a las unidades en esa materia se ha mantenido hasta la fecha, es simplemente cuestión de que el nivel local nos solicite nuestro criterio."

Lo evidenciado en el presente hallazgo podría ocasionar el no mantener en óptimo estado el funcionamiento de los equipos de redes y comunicaciones, lo anterior por la ausencia de lineamientos que regulen aspectos en torno a la administración estandarizada de estos dispositivos y que aseguren razonablemente la disponibilidad y resolución oportuna de incidentes, sin generar atrasos o limitaciones en la obtención de los resultados o productos esperados.

2. SOBRE LA DOCUMENTACIÓN DE RESPALDO EN LA GESTIÓN DE LA CONFIGURACIÓN

Se identificaron debilidades sobre la documentación o mecanismos utilizados para evidenciar las acciones efectuadas en torno a la gestión de configuración de los equipos de redes y comunicaciones, lo anterior por parte de Centros de Gestión Informática Regionales y Locales[1], en aspectos como:

- Ausencia de diagramas de red.
- Documentación desactualizada sobre la infraestructura de redes y comunicaciones.
- Identificación de las redes de área local virtuales (VLAN por sus siglas en inglés), únicamente se dispone accediendo a la consola de administración de los equipos.
- Falta de documentación de las configuraciones efectuadas sobre los equipos.
- Controles en herramientas ofimáticas de los equipos de redes y comunicaciones los cuales se orientan más a tareas de inventario y no de su configuración.

Las Normas de Control Interno para el Sector Público, en su capítulo 4.2 requisitos de las actividades de control, punto e, indica lo siguiente:

"Las actividades de control deben reunir los siguientes requisitos:

e. Documentación. Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación"

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Comunicaciones y Redes Informáticas establece:

(…) Asesorar y evaluar los Centros de Gestión Informática, en atención a la regulación y normativa vigente, los protocolos, estándares, políticas y estrategias, en su ámbito de competencia, con la finalidad de lograr el desarrollo efectivo y verificar el cumplimiento de los lineamientos establecidos.

[1] Dirección de Red Integrada Prestación de Servicios de Salud Chorotega, Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte, Hospital Dr. Enrique Baltodano Briceño, Área de Salud Buenos Aires de Puntarenas.

El Modelo de Organización de los Centros de Gestión Informática (octubre 2013) consigna como actividad sustantiva para los CGI Tipo B lo siguiente:

"Documentar e implementar la política de seguridad de la información, con base en la regulación y la normativa vigente, con el objeto de lograr confiabilidad: física y ambiental, en las operaciones y las comunicaciones, el control del acceso, la implementación, el mantenimiento de software e infraestructura tecnológica y la continuidad de los servicios, entre otros aspectos.

(…) Establecer los controles requeridos considerando: el acceso a las instalaciones, la ubicación física segura de los recursos, el ingreso y salida de los equipos, los servicios de mantenimiento, la seguridad del suministro de energía eléctrica, del cableado de datos, de las comunicaciones inalámbricas y de los riesgos asociados con el ambiente, de acuerdo con la normativa vigente, con la finalidad de asegurar la operación fluida de la gestión y la continuidad de los servicios."

El MSc. Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas, refiriéndose al equipamiento dotado por la Direccion del Expediente Digital Único en Salud, indicó lo siguiente:

"(…)recordemos que en el tema de parámetros o la configuración a efectuarse entraría como parte de la administración local de cada CGI, quienes a partir de su expertiz gestionan lo que estimen pertinente.

Eventualmente en el caso que presenten fallas esa instancia nos contacta para brindar colaboración en lo correspondiente.

Respecto a las condiciones o parámetros que deben de considerarse en equipamiento de acceso inalámbrico, no disponemos de documentación que apoye al nivel local sobre la configuración o elementos propios de la adquisición de ese tipo de dispositivos, no obstante, hemos visto la necesidad de implementar en esos niveles soluciones más corporativas y administradas, inclusive ya adquirimos una plataforma de administración para gestionar los equipos en los cuales se han implementado (7 sitios adicionales a los 2 edificios de oficinas centrales) este tipo de tecnología, además es posible que mediante esta forma se controle la configuración desde acá.

Ahora bien, este tipo de estrategia lo que busca es obviar totalmente la adquisición de access point "caseros" y poco a poco ir considerando dentro del contrato de access point a demanda a otras unidades externas, esperamos seguir bajo ese modelo, en aras de estandarizar lo correspondiente y así obtener mayores beneficios para la Institución.

Inclusive se busca en esa misma línea, que se estimen las necesidades de redes y comunicaciones en los sitios y paulatinamente ir estandarizando la adquisición de equipos de redes.

Eventualmente obteniendo la estandarización sobre la administración y monitoreo que se podría aplicar a los dispositivos, claro esta que esta iniciativa viene empezando y se efectuaría paulatinamente, recordemos que se ha invertido recientemente en equipamiento EDUS y estos no serían objeto de esta estrategia en el corto plazo y en otros casos existen equipos con contratos vigentes y/o en garantía."

(…) Este tema lo vemos como una posibilidad de estandarizar lo correspondiente a la gestión de la configuración, lo cual es un tema que no se encuentra definido aún, al menos para equipo de redes y comunicaciones, y aunque a veces desearíamos brindar más colaboración en el nivel local, nuestro ámbito de acción y la capacidad instalada, nos limita para atender oportunidades de mejora relacionadas al tema."

Al respecto, el Licda. Jeannette Madrigal Loría, Jefe Subárea Soporte a Comunicaciones, refiriere al tema, lo siguiente:

"nosotros como área no tenemos un documento que indique que direcciones IP se deben utilizar, VLAN, puertos u otros elementos a configurar en los equipos a nivel interno, ya que consideramos que esto le corresponde al cada administrador de la red, como parte de su función sustantiva. No obstante, si recomendamos algunos aspectos a considerar dentro de la distribución (como tipo especificación) que debería de tenerse a lo interno, esto basado en nuestra experiencia, la cual adquiere connotación de asesoría y/o recomendación.

Es importante mencionar que, al momento de implementar una red, el área de redes y comunicaciones simplemente brinda apoyo a las unidades programáticas, sin embargo, cada uno de los sitios son los que establecen las condiciones y características de su red, considerando que ellos son los que conocen las necesidades y realidades de sus áreas de trabajo, por ejemplo, la cantidad de equipos que disponen, la cantidad de servidores implementados, los servicios que brindan entre otros aspectos a considerar.

Recordemos que muchas de estas labores propias de configuración son delegadas en los proveedores, ya que en las condiciones del cartel se especifica se debe instalar y probar los dispositivos."

La ausencia de documentación que respalde las labores efectuadas sobre la configuración y distribución de los equipos de telecomunicaciones podría afrontar riesgos asociados a desconocer la referencia utilizada para alinear los dispositivos a la funcionalidad establecida en cada sitio de trabajo, situación que ante la necesidad de diagnosticar o restablecer un servicio, afectaría la utilidad o garantía de brindar continuidad a la infraestructura tecnológica.

3. SOBRE LAS HERRAMIENTAS PARA MONITOREAR LAS CONFIGURACIONES EN EQUIPAMIENTO

Este Órgano Fiscalizador identificó la ausencia de herramientas de monitoreo establecidas para determinar la integridad de la configuración actual de los equipos de redes y comunicaciones, de manera que se consulte los eventos ocurridos o se prevengan cambios no autorizados, lo anterior de acuerdo con lo indicado por la administración, tal y como se observa a continuación:

Tabla 1. Observaciones relacionadas con el monitoreo para verificar la integridad de la configuración

Entrevistado	Observaciones
Lic. Douglas Antonio Marín Mendoza, encargado de informática de la Dirección de Red Integrada Prestación de Servicios de Salud Chorotega	"No se disponen de herramientas destinadas para estos efectos, en caso de estimarse necesario se debe solicitar al ACRI que revise el estado de la red, mediante un escaneo. No se disponen de estos equipos o herramientas para monitorear o prevenir este tipo de incidencias, nos enteraríamos por el nivel central (sin embargo, desconozco si existe un monitoreo periódico por parte de la DTIC para identificar estas incidencias) o se reportaría en caso a lo Meso de Servicios para solventar algún problema relacionado."
Lic. Rafael Ángel Álvarez Rodríguez, CGI del Dirección Regional de Sucursales.	"A nivel local no disponemos de herramientas destinadas para esos efectos, en algún momento se solicitó este tipo de herramientas para monitorear los enlaces, anchos de banda, saturaciones en la red, entre otros, no obstante, no fructifico la solicitud."
Lic. Jimmy Ortiz Duarte, coordinador CGI de la Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte	"No se disponen de herramientas destinadas para estos efectos, lo más cercano es la herramienta Advance iP Scanner, en caso de estimarse un requerimiento de mayor complejidad lo gestionamos ante el ACRI."
Ing. Jency Alpízar Rodríguez, Jefe del CGI del Hospital San Vito	"No se nos ha suministrado una herramienta, y hemos consultado a la Mesa de Servicios TIC sobre la posibilidad de utilizar una de uso gratuito, sin embargo, no hemos obtenido respuesta."
Jimmy Andrés Salazar Arrieta, Coordinador CGI del Hospital de San Carlos	"En este caso prevalecen las políticas que puedan definirse por el nivel central para equipos finales (como medida de seguridad), ya que desde mi ámbito no realizo acciones orientadas a monitoreo o administración de configuraciones."
Licda. Carmen Suarez González, Jefatura del CGI del Hospital de San Ramón	"Importante mencionar que debe existir mayor apertura a capacitación para atender las condiciones y requerimientos del Hospital. Adicionalmente disponer de herramientas que apoyen el monitoreo y observancia de la continuidad de estos."

Fuente: Elaboración propia con la información de las entrevistas aplicadas, 2019

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el capítulo IV, punto 4.2. sobre Administración y Operación de la Plataforma Tecnológica, indica lo siguiente:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: (…)*
>
> *b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
> *c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.*
> *d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.*
> *e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.*
> *f. Mantener separados y controlados los ambientes de desarrollo y producción."*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Comunicaciones y Redes Informáticas establece:

"Planificar la adquisición de las tecnologías de información y las comunicaciones en su ámbito de acción, a partir de los requerimientos institucionales y los nuevos avances en la materia, con el propósito de contar con las herramientas necesarias que permiten atender con oportunidad las demandas de los usuarios.

Monitorear la infraestructura de redes inalámbricas y de voz, con base en los planes establecidos, para lograr un funcionamiento efectivo de la gestión de las unidades de trabajo de la Institución.

Monitorear la infraestructura de redes alámbricas, con base en los requerimientos institucionales, con el propósito de garantizar su correcta operación."

El Modelo de Organización de los Centros de Gestión Informática (octubre 2013) consigna como actividad sustantiva para los CGI Tipo B lo siguiente:

"Administrar los dispositivos de comunicaciones en su ámbito de acción, conforme con las políticas y estándares definidos, con el propósito de asegurar la comunicación efectiva de los sistemas de información."

(…) Verificar en su ámbito de competencia la disponibilidad, capacidad, desempeño y uso de la plataforma tecnológica, mediante la aplicación de procedimientos y responsabilidades asociadas, con el objeto de asegurar la operación eficaz y mantener un registro de eventuales fallas.

(…) Vigilar constantemente el desempeño y la suficiencia de la plataforma tecnológica (hardware y software) en su ámbito de competencia, mediante la aplicación de la normativa vigente, con el fin de minimizar la interrupción parcial o total de los servicios y evitar la pérdida económica y de imagen institucional."

El MSc. Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas, refiriéndose a la administración y seguimiento a los equipos, indicando lo siguiente:

"administramos la red LAN/WLAN de oficinas centrales, y los enlaces WAN a nivel Institucional.

En lo que respecta a esa responsabilidad sobre los enlaces WAN, se delega parcialmente la administración en un proveedor, ya que existe una figura de servicios administrados el cual brinda la cobertura por ese concepto, siendo de esta manera, el ICE es el que realiza la gestión de la configuración como parte del servicio adquirido, dicho contrato incluye tanto los enlaces como los equipos de borde existentes a nivel Institucional.

Para el caso del equipamiento que se encuentre fuera del servicio supra citado, estos son administrados desde el nivel local y en caso de requerirse nuestra intervención existe una comunicación directa con nosotros para coordinar lo correspondiente al apoyo técnico que se requiera en el CGI que solicita nuestra atención para acceder a sus equipos y efectuar revisiones, entre otras actividades.

En cuanto equipamiento de telefonía este tema ahora es gestionado directamente por la DTIC, debido que esa Direccion tramitó un contrato para el servicio de comunicaciones unificadas."

La falta de herramientas para monitorear la configuración de los equipos de manera preventiva podría materializar riesgos referentes a la disponibilidad, capacidad, desempeño y uso de los dispositivos de telecomunicaciones en las unidades programáticas, debido al menoscabo de las labores orientadas a identificación, cambios desautorizados y ajustes que puedan provocar interrupciones parciales o totales de los servicios.

4. SOBRE LOS PRIVILEGIOS DE ACCESO PARA GESTIONAR LA CONFIGURACIÓN

Este Ente Fiscalizador identificó vulnerabilidades de seguridad informática , la cual constituye un atributo relevante en la gestión de la configuración en equipamiento de redes y comunicaciones. A continuación, se detalla lo mencionado:

- Existen equipos que disponen de contraseñas de acceso establecidas por el fabricante y no han sido modificadas, lo cual expone a vulnerabilidades asociadas a la seguridad de la red Institucional.

- La administración de la configuración en los equipos se efectúa por medio de un único perfil, utilizado por usuarios internos y externos, es decir, esa contraseña podría ser de conocimiento para el personal experto en el nivel central de la CCSS, funcionarios del Centro de Gestión Informática y proveedores contratados.

A continuación, las observaciones efectuadas por los CGI, relacionado a los aspectos antes mencionados:

Tabla 2. Observaciones relacionadas con el manejo de contraseñas en equipo de redes y comunicaciones

Entrevistado	Observaciones
Lic. Douglas Antonio Marín Mendoza, encargado de informática de la Dirección de Red Integrada Prestación de Servicios de Salud Chorotega	"Para los equipos que me consulto. Activo No. 836102 y 836103 referenciados o lo ip No. 10.30.1.3; Activo No. 836104 ip No. 10.30.1.4, efectivamente están configurados con el usuario "admin" y contraseña "admin", los cuales fueron asignados de fabrica por el proveedor."
Lic. Jimmy Ortiz Duarte, coordinador CGI de la Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte	"En algunos equipos se han considerado, pero existen equipos actualmente que tienen contraseñas y/o configuraciones por defecto."
Ing. John Harold Vega Gómez, jefe del CGI del Hospital Cuidad Neilly	"Para ser sincero no se han establecido contraseñas seguras, los usuarios y contraseñas en los equipos utilizan las definidas por defecto Admin/Admin. En cuanto el switch de core la contraseña solamente la dispone el proveedor y no es de mi conocimiento."
Jimmy Andrés Salazar Arrieta, Coordinador CGI del Hospital de San Carlos	"No han sido consideradas, en el entendido de que los equipos son de tecnología obsoleta y por ende no tienen interfaces de administración."
Alvaro Alvarado Espinoza, encargado del CGI del Área de Salud de Tilarán	"Se configuraron para accesar mediante un único usuario y contraseña que se definió por mi persona, adicionalmente el direccionamiento es estático para asegurarnos su acceso seguro."

Fuente: Elaboración propia con la información de las entrevistas aplicadas, 2019

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el apartado 1.4 Gestión de la seguridad de la información, se cita lo siguiente:

"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
- La continuidad de los servicios de TI.

Además debe establecer las medidas de seguridad relacionadas con:

- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal."

En ese mismo cuerpo normativo, específicamente en el apartado 1.4.2 Compromiso del personal con la seguridad de la información, cita lo siguiente:

"El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.

Para ello, el jerarca, debe:
a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos."

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Comunicaciones y Redes Informáticas establece:

"Generar cultura informática en su ámbito de acción, conforme con los programas de capacitación, divulgación y concienciación, a efecto de facilitar y promover el uso de la tecnología disponible y lograr un desarrollo tecnológico institucional articulado.

(…) Aplicar de la regulación y la normativa técnica de seguridad y calidad, con base en los estándares institucionales, las políticas y las estrategias vigentes, con la finalidad de proteger los sistemas de información institucionales, promover la confiabilidad y la continuidad en la prestación de los servicios."

El Modelo de Organización de los Centros de Gestión Informática (octubre 2013) consigna como actividad sustantiva para los CGI Tipo B lo siguiente:

"Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios), con base en los procedimientos de requisición, aprobación, establecimiento, suspensión y desactivación de los medios, con el fin de identificar y responsabilizar a quienes utilizan los recursos de tecnologías de información."

Las Normas Institucionales de Seguridad Informática, indican en el numeral "6.1. Normas para la política correcto uso de contraseñas de parte de los usuarios de red y aplicaciones" que:

"Todo funcionario de la red institucional y de aplicaciones, que posea una o varias cuentas creadas a su nombre, deberá cumplir con las siguientes normas, que constituyen las mejores prácticas para la manipulación de las contraseñas personales y lo protegerán del hurto y modificación de la información institucional que administra.
1. Queda estrictamente prohibido a los funcionarios de la Institución utilizar sus cuentas de usuario para obtener cualquier clase de beneficio propio y/o para terceros.
2. La contraseña no deberá compartirse, sin excepción con ninguna otra persona (aunque se trate de la jefatura, un soportista, o compañeros de trabajo), ya que el dueño de la cuenta será el responsable por el uso que se le dé a la misma.
3. El usuario no debe dejar contraseñas escritas en medios o lugares donde puedan ser accesados por terceros (por ejemplo, en una carpeta del escritorio, en la pantalla del equipo, debajo del teclado u otros).
4. El usuario estará enterado que después de ejecutar tres intentos fallidos de "logueo" en su cuenta de red y o de aplicaciones, la misma será bloqueada, esto para proteger sus datos e identidad, en caso de olvidar definitivamente la contraseña, deberá solicitar la activación de la misma ante su respectivo administrador, en persona y aportando alguna identificación como medida para corroborar su identidad o por otra parte puede enviar una nota o formulario previamente diseñado para esta labor con la firma y sello correspondiente por parte de la Jefatura respectiva, dicha nota debe estar dirigida al administrador del CGI respectivo.
5. Todo usuario deberá hacer el cambio periódico de sus contraseñas cada (tres) 3 meses como mínimo.
6. Las contraseñas generadas por los usuarios para su uso en los servicios de red y aplicaciones, deben contener caracteres de al menos (tres) 3 de las siguientes (cuatro) 4 clases:

Clase	Descripción de la clase
Letras mayúsculas	A, B, C, . . . Z.
Letras minúsculas	a, b, c, . . . z.
Números	0, 1, 2,. . . 9.
Caracteres especiales	Por ejemplo: Símbolos puntuación ú otros como % & ¡ @ ( ) .

7. Todo usuario deberá tomar en cuenta las siguientes restricciones, que han sido configuradas para que las contraseñas sean más seguras:
• La longitud de toda contraseña a utilizar deberá ser igual o mayor a ocho caracteres.
• La contraseña a adoptar no podrá ser igual o similar a su respectivo nombre de usuario.
• No podrá repetir ninguna de las últimas seis contraseñas utilizadas.
• No se podrá dejar contraseñas en blanco."

Al respecto, el MSc. Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas, refiriéndose a la actualización de la normativa existente, indicó lo siguiente:

"para el manejo del respaldos, contraseñas seguras y medidas de seguridad en los accesos, el área de seguridad informática ha emitido documentación que refiere el tema, por tanto, nosotros no hemos establecido ningún lineamiento de ese tipo. Al respecto podríamos considerarnos, usuarios de esos procedimientos establecidos por parte del área supra citada.

(…) lo ideal es no permitir el establecimiento y uso de usuarios genéricos, con el objetivo de identificar quien entró y en qué momento lo hizo, por ello se debe aplicar las normas establecidas a nivel de seguridad informática, con el objetivo de evitar riesgos o vulnerabilidades en equipos de comunicaciones.

Además, una recomendación que podría ser de utilidad en las unidades externas es el accesar a los equipos por medio de los usuarios definidos a nivel institucional (definidos en el AD), de esa manera regulando quien ingresa y a su vez monitoreándolo; al menos nosotros en el nivel central estamos en proceso de implementarlo, como una iniciativa que pretende dar valor agregado a la administración de los equipos."

El incumplimiento de prácticas de seguridad en TIC en equipos de telecomunicaciones podría afectar la obtención de garantías razonables sobre la integridad de la configuración efectuada y la disponibilidad de los equipos, debido a la vulnerabilidad a la que se exponen estos dispositivos a una posible alteración de parámetros o accesos no autorizados provocando daños al hardware y software, así como interrupciones de los servicios tecnológicos.

5. SOBRE LOS RESPALDOS DE LA CONFIGURACIÓN DEL EQUIPAMIENTO

Se evidenció la ausencia de respaldos o repositorios destacados exclusivamente para contener toda la información relevante sobre los ítems de configuración de los equipos de redes y comunicaciones, a fin de identificar los puntos de restauración generados, parámetros utilizados, diseños de red, entre otros elementos propios de esa gestión, esto como parte del efecto generado ante la ausencia de lineamientos específicos sobre el tema.

Por otra parte, se identificó de manera generalizada en las unidades programáticas diferentes medios de almacenamiento para efectuar los respaldos, así como la periodicidad variable al crearlos, no obstante, la misma administración reconoce oportunidades de mejora en cuanto la disponibilidad, confiabilidad e integridad de la información supra citada, la cual podría apoyarse en lineamientos específicos para obtener los objetivos plasmadas para esas actividades.

Tabla 3. Observaciones relacionadas con los respaldos de la configuración en equipo de redes y comunicaciones

Entrevistado	Observaciones
Lic. Jimmy Ortiz Duarte, coordinador CGI de la Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte	"Actualmente no se disponen de rutinas para realizar respaldos, a futuro en las condiciones cartelarlas lo vamos a incluirlo para mitigar los riesgos asociados. No disponemos de un repositorio para tales efectos, en el entendido que no hemos realizado respaldos de la configuración de los equipos que tenemos"
Ing. John Harold Vega Gómez, jefe del CGI del Hospital Cuidad Neilly	"Los respaldos de los equipos los realizo por mi parte, tengo una carpeta local en mi computador y ahí coloco la última versión del respaldo, remplazando la versión anterior."
Jimmy Andrés Salazar Arrieta, Coordinador CGI del Hospital de San Carlos	"No se disponen de rutinas programadas o respaldos propiamente realizados con la configuración de los equipos."

Fuente: Elaboración propia con la información de las entrevistas aplicadas, 2019

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el capítulo IV, punto 4.2. sobre Administración y Operación de la Plataforma Tecnológica, refieren lo siguiente respecto al tema:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: (…)*
>
> *h. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración."*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Comunicaciones y Redes Informáticas establece:

> *"Generar cultura informática en su ámbito de acción, conforme con los programas de capacitación, divulgación y concienciación, a efecto de facilitar y promover el uso de la tecnología disponible y lograr un desarrollo tecnológico institucional articulado.*
>
> *(…) Aplicar de la regulación y la normativa técnica de seguridad y calidad, con base en los estándares institucionales, las políticas y las estrategias vigentes, con la finalidad de proteger los sistemas de información institucionales, promover la confiabilidad y la continuidad en la prestación de los servicios."*

El Modelo de Organización de los Centros de Gestión Informática (octubre 2013) consigna como actividad sustantiva para los CGI Tipo B lo siguiente:

> *"Definir y realizar las rutinas de respaldo, custodiar los mismos en ambientes seguros, con base en las políticas y los procedimientos de control requeridos, con la finalidad de mantener la plataforma tecnológica en óptimas condiciones y minimizar los riesgos."*

Según la Guía técnica para gestión de procesos de mantenimiento preventivo y correctivo en routers y switches, TIC-COM-0003, Versión 1.0.0 Octubre 2014, se incluye en el inciso 2 "condiciones generales", lo siguiente:

> *"e. Previo al desarrollo del proceso mantenimiento, se debe considerar la ejecución de respaldos del sistema operativo, configuraciones u otros elementos que se consideren importantes."*

Al respecto, el MSc. Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas, refiriéndose a la actualización de la normativa existente, indicó lo siguiente:

> *"para el manejo del respaldos, contraseñas seguras y medidas de seguridad en los accesos, el área de seguridad informática ha emitido documentación que refiere el tema, por tanto, nosotros no hemos establecido ningún lineamiento de ese tipo. Al respecto podríamos considerarnos, usuarios de esos procedimientos establecidos por parte del área supra citada."*

Los respaldos sobre la configuración de los equipamientos de telecomunicaciones funcionan como medida de contingencia para garantizar medios de restauración ante eventuales interrupciones al servicio. Debido a su ausencia, se podría comprometer la continuidad en los servicios tecnológicos en caso de fallas, afectando el rendimiento de los sistemas de información y, por ende, la prestación de servicios que automatizan esas soluciones.

6. SOBRE LA RUTINAS DE MANTENIMIENTO ASOCIADAS A LA GESTIÓN DE LA CONFIGURACIÓN

Se evidenciaron oportunidades de mejora en relación con la gestión de la configuración presente en los mantenimientos aplicados a equipos de redes y comunicaciones, lo anterior, considerando la documentación que respalda las acciones efectuadas por los proveedores, así como las actividades ejecutadas como parte de las rutinas definidas para los dispositivos, destacando los siguientes aspectos:

- En siete Centros de Gestión Informática[2], se evidenció que, en los mantenimientos preventivos y correctivos efectuados por los proveedores, no se indica en los reportes el detalle de las tareas concernientes a la gestión de configuración aplicadas en los dispositivos, evidenciándose riesgos sobre la calidad de los datos contenidos en los mecanismos de control destinados para tales fines.

[2] Área de Salud de Coto Brus, Dirección Regional de Sucursales Brunca, Hospital Dr. Tomás Casas Casajus, Hospital de San Carlos, Hospital Cuidad Neilly, Hospital San Vito, Hospital Dr, Enrique Baltodano Briceño

- En el caso de la Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte y el Hospital de San Carlos se determinó que la gestión de mantenimiento preventivo efectuada por los CGI se limita únicamente a limpieza externa de los equipos de telecomunicaciones.

Al respecto, es significativo mencionar que según el Área de Comunicaciones y Redes Informáticas, se ha insistido a la unidades locales en prestar atención a las condiciones referentes al mantenimiento preventivo y correctivo que se efectúan en los equipos de telecomunicaciones, prueba de ello es la "Guía técnica para gestión de procesos de mantenimiento preventivo y correctivo en routers y switches", la cual pretende crear conciencia en esas tareas, disminuyendo con ello la obsolescencia y fallas en los dispositivos que puedan ocasionar incidencias.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el capítulo IV, punto 4.2. sobre Administración y Operación de la Plataforma Tecnológica, indica lo siguiente:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: (…)*
>
> *e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro."*

El Modelo de Organización de los Centros de Gestión Informática (octubre 2013) consigna como actividad sustantiva para los CGI Tipo B lo siguiente:

> *"… Programar en forma periódica el mantenimiento preventivo para el hardware, el software y las comunicaciones, con base en las políticas y normas institucionales vigentes, con el fin de lograr la eficiencia, la eficacia y la productividad de la gestión.*
>
> *Establecer mecanismos de control de calidad, de oportunidad, de seguridad, entre otros, de servicios contratados a terceros, con base en la regulación y la normativa técnica, con la finalidad de lograr la efectividad de la gestión…".*

Según la Guía técnica para gestión de procesos de mantenimiento preventivo y correctivo en routers y switches, TIC-COM-0003, Versión 1.0.0 Octubre 2014, se incluye en el inciso 4 "Seguimiento y condiciones recomendadas para el mantenimiento preventivo y correctivo", lo siguiente:

> *"A continuación se detalla una serie de elementos que deben ser considerados para la gestión de un proceso de mantenimiento:*
>
> *a. El primer mantenimiento preventivo para los equipos se debe realizar según se establece en el contrato de mantenimiento o programación pertinente. Los siguientes mantenimientos se realizan de acuerdo a las necesidades propias de cada unidad de trabajo, de forma mensual, trimestral, semestral o según lo establezca el interesado.*

b. Se debe establecer un responsable para la coordinación de la ejecución de los procesos de mantenimiento de los equipos, quien debe coordinar los respectivos permisos en caso que corresponda.

c. Si el mantenimiento es contratado o realizado por personal informático de la unidad o un CGI, se debe presentar a la jefatura respectiva un informe de las actividades realizadas durante el proceso, considerando un plazo no mayor a 7 días hábiles posteriores a la fecha de realizado para la entrega del mismo.

d. La ejecución de los procesos de mantenimiento, las pruebas y la recepción definitiva de los mismos, se encuentran a cargo del colaborador designado para tales efectos.

e. El proceso de reporte de fallas se realiza informando al contratista de la avería, la misma se debe reportar al contratista vía telefónica, al número que se indique como referencia para la atención de incidentes. El proveedor debe asignar un número de reporte el cual es informado a la jefatura por el medio definido en la oferta adjudicada."

La Licda. Sirleny Barrantes Valverde, CGI del Área de Salud de Coto Brus, en entrevista efectuada, indicó lo siguiente:

"Las rutinas son las establecidas según las condiciones de los pliegos cartelarios, en ocasiones el proveedor anota el detalle de las acciones realizadas, pero por lo general se anota de forma generalizada."

El Ing. Jorge Paniagua Pérez, Jefe del Area de Gestión Informática Dirección Regional de Sucursales Brunca, indicó lo siguiente:

"(..) las actualizaciones se realizan en visitas realizadas a unidades, pero no se profundiza el detalle técnico en los informes presentados a la administración activa."

El Ing. John Harold Vega Gómez, jefe del CGI del Hospital Cuidad Neilly, menciono sobre el tema:

"Corroboro que sea funcional, no obstante, no tengo documentación que apoye mi gestión para poder corroborar, recordemos que la empresa de FONT tiene muchas contrataciones relacionadas a esos ámbitos y conocen cuales son las configuraciones que deben tener los equipos."

"El proveedor realiza el mantenimiento, no obstante, no se indican en los reportes detalles sobre la configuración que tienen los mismos o sobre los cambios que se han realizado."

La Ing. Jency Alpízar Rodríguez, Jefe del CGI del Hospital San Vito, indicó al respecto:

"No se hace alguna verificación específica al respecto, básicamente se revisa que haya conectividad."

Aspectos como los señalados en el presente hallazgo podrían comprometer la prestación de los servicios de mantenimiento de los dispositivos citados, tanto por la ausencia de respaldo documental, evidencia sobre las actividades ejecutadas en el sitio y finalmente la omisión en la ejecución de otras acciones necesarias, esto ocasionando la materialización de riesgos asociados a la probabilidad de fallos u operaciones contrarias al buen funcionamiento de los equipos.

7. SOBRE LA CAPACITACIÓN EN TEMAS RELACIONADOS A GESTIÓN DE LA CONFIGURACIÓN DE EQUIPOS DE TELECOMUNICACIONES

Se determinó oportunidades de mejora en torno a la capacitación institucional en el tema de gestión de la configuración para equipamiento de redes y comunicaciones, evidenciándose los siguientes riesgos:

- A partir de los resultados obtenidos en consulta efectuada a 15 CGI de unidades programáticas destacadas en el I, II y III nivel de atención, redes integradas de prestación de servicios de salud y de sucursales financieras, se indicó por los funcionarios entrevistados que no han sido capacitados específicamente y/o recientemente en el tema de configuración de equipamiento de telecomunicaciones y por ende en la gestión a efectuarse en ese tipo de dispositivos.

Tabla 4. Observaciones relacionadas capacitación sobre gestión de la configuración en equipo de redes y comunicaciones

Entrevistado	Observaciones
Lic. Douglas Antonio Marín Mendoza, encargado de informática de la Dirección de Red Integrada Prestación de Servicios de Salud Chorotega	"Se recibió capacitación de CISCO aproximadamente 4 años, pero estas capacitaciones son orientadas a un mercado especifico y sin necesariamente ajustarse a las realidades de los Centros de Gestión en Informático."
Ing. Herschel Alberto Jiménez Barahona, jefe del CGI del Area de Salud de Naranjo	"De parte de la institución nunca he recibido una capacitación formal en materia de redes de comunicación pese a que si han convocado a otros colegas sobre todo de Clínicas mayores y Hospitales."
Ing. Rafael Porras Murillo, jefe del CGI del Hospital Dr. Tomás Casas Casajus	"No se ha recibido capacitación al respecto, lo más cercano o capacitación es los cursos de CCNA (inaplicable a nuestra realidad en visto de que tenemos otros equipos de distinta marca) que realice hace 2 años, adicional a la que se recibe por parte de los proveedores al momento de la entregada de los equipos adjudicados a la unidad."
Ing. Jency Alpízar Rodríguez, Jefe del CGI del Hospital San Vito	"No, a pesar de que se ha solicitado en varias ocasiones tanto a nivel local, regional y central."

Fuente: Elaboración propia con la información de las entrevistas aplicadas, 2019

- Existen labores de configuración aplicadas de manera empírica en los equipos de telecomunicaciones por parte de CGI's, los cuales podrían no ser acordes a las necesidades o servicios requeridos a nivel Institucional, según se puede apreciar en la siguiente tabla:

Tabla 5. Observaciones relacionadas con la configuración de equipo de redes y comunicaciones

Entrevistado	Observaciones
Lic. Alvaro Alvarado Espinoza, CGI del Área de Salud de Tilarán	"No se dispone de procedimientos definidos en el nivel local y no tenemos conocimiento de documentos elaborados por el nivel central de la CCSS que apoye la gestión que se debe realizar para configurar los equipos. En lo que respecta a equipamiento dotado por los compañeros del EDUS, los equipos de telecomunicaciones se encuentran en gabinete bajo llave, y por tanto no se tiene acceso para realizar configuraciones, estos equipos son administrados totalmente por el ICE."
Lic. Douglas Antonio Marín Mendoza, encargado de informática de la Dirección de Red Integrada Prestación de Servicios de Salud Chorotega	"los puntos de acceso inalámbricos que disponemos son 5, han sido configurados por mi persona, estableciendo la configuración que consideré necesaria para su funcionamiento, en el entendido de que no hay ninguna directriz de como configurarlos."
Lic. Jimmy Ortiz Duarte, coordinador CGI de la Dirección de Red Integrada Prestación de Servicios de Salud Huetar Norte	"configurados por mi persona, estableciendo la configuración que consideré necesaria para su funcionamiento, en el entendido de que no hay ninguna directriz de como configurarlos, inclusive en días atrás personal de EDUS realizaron una visita para verificar su uso y al consultarles estos no tenían una configuración establecida para los equipos, más bien creo que ellos replicaron la configuración que nosotros utilizamos debido o que funcionaba de manera adecuada."
Licda. Sirleny Barrantes Valverde, CGI del Área de Salud de Coto Brus	" No dispongo de manuales para configurar los puntos de acceso inalámbrico, de hecho, he tenido problemas porque no tenía conocimiento para configurarlos, hemos dependido de otros compañeros que me orientaron para lograr ponerlos en funcionamiento. Estos equipos que me refiero fueron dotados por el proyecto EDUS, no obstante, nosotros asumimos la configuración y la puesta en marcha de los equipos."

Fuente: Elaboración propia con la información de las entrevistas aplicadas, 2019

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones establece en el apartado 5.7.1 "Nivel: Dirección ", lo siguiente:

> *"(…) Promover el desarrollo de programas de capacitación y actualización profesional de los funcionarios, según los requerimientos y necesidades de la organización, con la finalidad de elevar los niveles de calidad y excelencia en la prestación de los servicios.*
>
> *Asesorar y coordinar actividades con los Centros de Gestión Informática, a partir de los requerimientos de la organización, la regulación y la normativa vigente, con el propósito de lograr el desarrollo efectivo de la gestión y la participación activa de estas unidades de trabajo. (…)"*

El Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, como función sustantiva del Área de Comunicaciones y Redes Informáticas establece:

"Establecer y coordinar los requerimientos de capacitación y de actualización profesional de los colaboradores, de acuerdo con las políticas institucionales y las necesidades de la organización, con la finalidad de contar con el personal idóneo para el desarrollo de la gestión.

Generar cultura informática en su ámbito de acción, conforme con los programas de capacitación, divulgación y conciencia, a efecto de facilitar y promover el uso de la tecnología disponible y lograr un desarrollo tecnológico institucional articulado.

El MSc. Sergio Porras Solís, Jefe del Área de Comunicaciones y Redes Informáticas, refirió al respecto:

"Solo se ha gestionado la solicitud de capacitación a nuestro personal, no obstante inclusive para nosotros se ha dificultado, por tanto esto representa una limitante para obtener o reforzar conocimiento en esos temas."

Si bien es cierto, los funcionarios del Centro de Gestión Informática reconocen que han generado conocimiento a partir de iniciativas propias, así como retroalimentación obtenida por otros medios, esta situación podría conllevar a una administración sobre la red de telecomunicaciones basada en diferentes configuraciones no optimizadas, esto ante la ausencia de capacitación y/o actualización profesional de los responsables de la red en cada unidad programática de la Institución.

CONCLUSIONES

Esta Auditoría en el desarrollo del presente estudio referente a la gestión de la configuración en equipo de redes y comunicaciones a nivel Institucional, evidenció oportunidades de mejora que deben considerarse con el propósito de garantizar la continuidad en la prestación de los servicios tecnológicos institucionales de manera oportuna y razonable.

En primera instancia, cabe mencionar que las telecomunicaciones a nivel mundial y particularmente en el ámbito nacional toman relevancia bajo la óptica del impacto al desarrollo de la tecnología en la TI, respecto a ello uno de los componentes a referirse en ese accionar corresponde a la configuración efectuada en los dispositivos de redes y comunicaciones, mediante los cuales es posible la prestación oportuna de los servicios asociados a las TIC.

En ese orden de ideas, la CCSS no se encuentra exenta sobre la estructura funcional de las telecomunicaciones conformada en la Institución, la cual debe estar sujeta a una adecuada gestión de la configuración aplicada al equipamiento que hace posible la interconectividad con la infraestructura tecnológica instalada, lo anterior, bajo criterios de eficiencia y eficacia equivalentes a la red que soporta.

Al respecto, los actores a nivel Institucional involucrados en la gestión de las redes y comunicaciones tienen oportunidades de mejora en cuanto administrar la configuración de los dispositivos, con el objetivo de garantizar su integridad, documentar la información vital de los ítems necesarios para poner en funcionamientos los equipos, así como disponer de respaldos que permitan minimizar eventuales riesgos asociados con la continuidad de los servicios soportados.

Bajo ese entendido, la formulación y/o actualización periódica de la normativa, así como el alineamiento entre marcos normativos, resultan prioritario en la Institución para garantizar una administración de la configuración con miras hacia la optimización de la infraestructura, recursos y capacidades de las Tecnologías de Información y Comunicaciones.

Asimismo, durante la evaluación se evidenció que el disponer de documentación referente a las acciones efectuadas en el nivel local y regional se debe mejorar, así como implementar herramientas de control y, supervisión que apoyen en ese ámbito, considerando el alcance sobre la administración de la red en las diferentes unidades programáticas, esto sin dejar de lado el aplicar prácticas de seguridad en TIC acorde con nuestra infraestructura de comunicaciones y redes informáticas.

Lo anterior es señalado por este Órgano Fiscalizador a fin de que la Administración Activa tome las consideraciones pertinentes en cumplimiento de lo establecido en la norma aplicable, en cuanto asesorar y evaluar los CGI, así como incentivar una cultura informática en materia de redes y comunicaciones, conforme con programas de capacitación, divulgación y concienciación de los aspectos a considerar en esta temática.

A continuación, se indican las siguientes recomendaciones en aras de abordar y subsanar los aspectos evidenciados en el presente informe.

RECOMENDACIONES

AL MÁSTER ROBERT PICADO MORA, EN SU CALIDAD DE SUBGERENTE DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES O A QUIEN EN SU LUGAR OCUPE SU CARGO.

1. De acuerdo con los riesgos identificados en el presente estudio, ejecutar un plan de acción con las actividades correspondientes para garantizar la gestión integral de la configuración en equipamiento de redes y comunicaciones en los diferentes ámbitos de operación de las TI a nivel Institucional asociados al tema, considerando al menos, los siguientes aspectos:

   a) Elaboración y/o actualización de marcos normativos institucionales asociados a la garantizar la gestión integral de la configuración así como su respectiva divulgación.
   b) Definición de mecanismos de control orientados a especificar la configuración aplicada en los equipos, considerando estandarizar la documentación que responde a este requerimiento.
   c) Definir mecanismos de monitoreo sobre la gestión de la configuración efectuada en equipamiento de redes y comunicaciones a fin de garantizar la continuidad de los servicios y la seguridad informática que corresponde a esta temática.
   d) Girar las instrucciones que estime pertinente para asegurar razonablemente el cumplimiento de la normativa vigente referente al establecimiento de contraseñas seguras, utilización de perfiles de acceso ajustados, disponibilidad de respaldos y gestión de mantenimientos, todo lo anterior aplicado a equipamiento de telecomunicaciones, entre otras situaciones propias de la administración que se puedan generar.
   e) Capacitación o socialización para el abordaje de los aspectos a considerar como parte de la temática supra citada, esto desde el ámbito que corresponda en las unidades programáticas de la Institución.

Para acreditar el cumplimiento de esta recomendación, debe remitirse a este Órgano de Fiscalización, en un plazo de 8 meses posterior al recibo del presente estudio, el plan de acción solicitado con el detalle de actividades, plazos y responsables del cumplimiento, así como el respaldo documental de su ejecución.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 16 de diciembre del 2019 con el Máster Christian Chacón Rodríguez, Sub Director de la Dirección de Tecnologías de Información y Comunicaciones. A continuación, se indican las observaciones realizadas en torno a los hallazgos y recomendaciones:

Sobre los Hallazgos: No hay observaciones.

Sobre las Recomendaciones: No hay observaciones.

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Firmado digitalmente por OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Fecha: 2019.12.17 13:58:31 -06'00'

Ing. Oscar Mena Granados
ASISTENTE DE AUDITORÍA

ESTEBAN ZAMORA CHAVES (FIRMA)
Firmado digitalmente por ESTEBAN ZAMORA CHAVES (FIRMA)
Fecha: 2019.12.17 13:56:21 -06'00'

Lic. Esteban Zamora Chaves
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2019.12.17 14:05:39 -06'00'

Lic. Rafael Herrera Mora
JEFE DE ÁREA

RAHM/OMG/edvz